Leonhard Euler (1707–1783).

theorem prover' was faced with the case of an arbitrary prime exponent.

The first person to make any real progress in this direction was Euler. In 1753, he claimed to have proved the result for $n = 3$. Though his published proof contained a fundamental flaw, the result is generally still credited to him. The problem with Euler's proof was that it depended upon a particular assumption about factorization that Euler made in the course of his argument. Though this assumption can in fact be proved for the case $n = 3$, it is not true for all prime exponents, as Euler seemed to be assuming, and in fact it was precisely this subtle, but invalid, assumption that brought down many subsequent attempts to prove Fermat's last theorem.

In 1825, extending Euler's argument, Peter Gustav Lejeune Dirichlet and Adrien-Marie Legendre proved Fermat's last theorem for exponent $n = 5$. (Their version of the argument avoided the factorization trap that befell Euler.)

Then, in 1839, using the same general approach, Gabriel Lamé proved the result for $n = 7$. By this stage, the argument was becoming increasingly intricate, and there seemed little hope of taking it any further, to deal with the next case, $n = 11$. (Not that this kind of piecemeal approach would solve the entire problem in any case.)

To make any further progress, what was required was the detection of some kind of general pattern in the proofs, a way of stepping back from the complexity of the individual trees to the larger-scale order of the forest. This advance was made by the German mathematician Ernst Kummer in 1847.

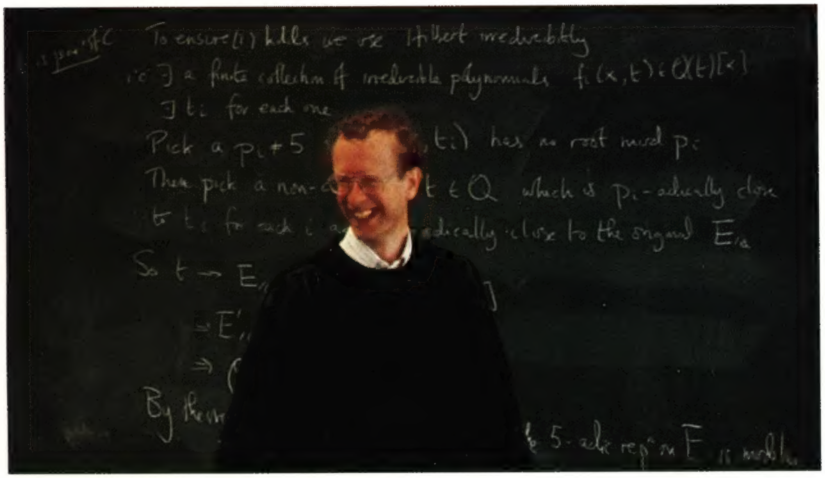
Kummer recognized that some prime numbers exhibited a certain kind of pattern, referred to by Kummer as *regularity*, which enabled an Euler-type proof of Fermat's last theorem to be carried through. Using this new property of regularity, Kummer was able to prove that Fermat's last theorem holds for all exponents n that are regular primes. Of the primes less than 100, only 37, 59, and 67 fail to be regular, so in one fell swoop Kummer's result established Fermat's last theorem for all exponents up to 36 and for all prime exponents less than 100 apart from 37, 59, and 67.

There are a number of different, but totally equivalent ways to define exactly what a regular prime is, but all refer to some fairly advanced mathematical concepts, so I will not give any definition here. What I will tell you is that computer searches as far as 4,000,000 have shown that most primes are regular.

Moreover, all the nonregular primes less than 4,000,000 satisfy a property a bit weaker than regularity, but which still implies Fermat's last theorem for that exponent. So Fermat's last theorem is known to be true for all exponents up to 4,000,000.

At which point, we must leave Fermat's last theorem, but only for the time being. We shall come back to it in Chapter 6, when I shall tell you about a startling discovery made in 1983, undoubtedly the

most significant advance on Fermat's last theorem subsequent to Kummer's work. I shall also tell you of dramatic events that took place in 1986 and 1993, which might well lead to final resolution of the three-hundred-year saga of Fermat's last theorem. The reason for putting off these two developments until later—indeed, several chapters later—is itself a striking illustration that mathematics is the search for, and study of, patterns. Both the 1983 discovery and the events of 1986 and 1993 only came about as a result of investigations of patterns of quite different natures—not number patterns but patterns of shape and position, patterns that involve the infinite in a fundamental way.



Andrew Wiles of Princeton University.

jects about which a great deal was known. Indeed, there was good reason to believe the result, and to suggest a way of setting about finding a proof. At least, the English mathematician Andrew Wiles saw a way to proceed.

For the next seven years, Wiles concentrated all his efforts into trying to find a way to make his idea work. Using powerful new methods developed by Barry Mazur, Matthias Flach, Victor Kolyvagin, and others, in 1993 he eventually succeeded in establishing the Shimura–Taniyama–Weil conjecture, not for all elliptic curves, but for a certain large class of elliptic curves.

Based on their understanding of the rich mathematical structures involved, many experts believe that the class of curves for which Wiles proof works includes those relevant to Fermat's last theorem. If this belief turns out to be correct, then Fermat's last theorem will be a theorem at last. But so far, no one has been able to prove this belief. Alternatively, it is possible that Wiles' argument has to be extended in order to apply to the relevant curves. Either way, it seems that the mathematical world is now within a hairsbreadth of ending a saga that began over three hundred years ago, with a comment scribbled by a French lawyer in the margin of a textbook.

The story of Fermat's last theorem is a marvellous illustration of humanity's never-ending search for knowledge and understanding. But it is much more than that. Mathematics is the only branch of science in which a precise, technical problem formulated in the seventeenth century, and having its origins in ancient Greece, remains as pertinent today as it did then. It is unique among the sciences in that a new development does not invalidate the previous theories, but builds on what has gone before. A long path leads from the Pythagorean theorem and Diophantus' *Arithmetic*, to Fermat's marginal comment, and on to the rich and powerful theory we have today, a theory that may result in a proof within the near future. A great many mathematicians have contributed to that development. They have lived (and are living) all over the world; they have spoken (and speak) many languages; most of them have never met. What has united them has been their love for mathematics. Over the years, each has helped the others, as new generations of mathematicians have adopted and adapted ideas of their predecessors. Separated by time, space, and culture, they have all contributed to a single enterprise. In this respect, perhaps mathematics can serve as an example to all humanity.